Please note that the following is the version that was approved by the NCUA Board. The official version is published in the Federal Register approximately one week after Board approval. There may be some minor numbering or format differences between the two versions.

7535-01-U

NATIONAL CREDIT UNION ADMINISTRATION

12 CFR Part 748

Security Program and Appendix A - Guidelines for Safeguarding Member Information.

AGENCY: National Credit Union Administration (NCUA).

ACTION: Notice of proposed rulemaking and request for comment.

SUMMARY: The NCUA Board is proposing a modification to the security program requirements to include security of member information. Further, the NCUA Board is requesting comment on proposed Guidelines for safeguarding member information published to implement certain provisions of the Gramm-Leach-Bliley Act (the GLB Act or Act).

The GLB Act requires the NCUA Board to establish appropriate standards for federally-insured credit unions relating to administrative, technical, and physical safeguards for member records and information. These safeguards are intended to: (1) insure the security and confidentiality of member records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any member.

DATES: NCUA must receive comments not later than [insert date 60 days after the publication date in the FEDERAL REGISTER].

ADDRESSES: Direct comments to: Becky Baker, Secretary of the Board. Mail or hand-deliver comments to: National Credit Union Administration, 1775 Duke Street, Alexandria, Virginia 22314-3428. You may fax comments to (703) 518-6319, or e-mail comments to boardmail@ncua.gov. Please send comments by one method only.

FOR FURTHER INFORMATION CONTACT: Matthew Biliouris, Information Systems Officer, or Jodee Jackson, Compliance Officer, Office of Examination and Insurance, at the above address or telephone (703) 518-6360.

SUPPLEMENTARY INFORMATION:

The contents of this preamble are listed in the following outline:

I. Background

On November 12, 1999, President Clinton signed the GLB Act (Pub. L. 106-102) into law. Section 501, entitled Protection of Nonpublic Personal Information, requires the NCUA Board, the federal banking agencies, including the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision, the Securities and Exchange Commission, state insurance authorities, and the Federal Trade Commission (collectively, the “Agencies”) to establish appropriate standards for the financial institutions subject to their respective jurisdictions relating to the administrative, technical, and physical safeguards for customer records and information. These safeguards are intended to: (1) insure the security and confidentiality of customer

records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that would result in substantial harm or inconvenience to any customer.

Section 505(b) of the GLB Act provides that these standards are to be implemented by the NCUA and the federal banking agencies in the same manner, to the extent practicable, as standards pursuant to section 39(a) of the Federal Deposit Insurance Act (FDIA). Section 39(a) of the FDIA requires the federal banking agencies to establish operational and managerial standards for insured depository institutions relative to, among other things, internal controls, information systems, and internal audit systems, as well as such other operational and managerial standards as determined to be appropriate. 12 U.S.C. 1831p(a). Section 39 of the FDIA provides for standards to be prescribed by guideline or by rule. 12 U.S.C. 1831p(d)(1). The FDIA also provides that, if an institution fails to comply with a standard issued as a rule, the institution must submit a compliance plan within particular time frames while, if an institution fails to comply with a standard issued as a guideline, the agency has the discretion as to whether to require an institution to submit a compliance plan. 12 U.S.C. 1831p(e)(1).

Section 39 of the FDIA does not apply to the NCUA, and the Federal Credit Union Act does not contain a similar, regulatory framework for the issuance and enforcement of standards. In preparation of NCUA's proposed regulation and appendix with guidelines,

NCUA staff has worked with an interagency group that has included representatives from the federal banking agencies. The NCUA Board's understanding is that the federal banking agencies intend to issue proposed standards by guidelines that will be published as an appendix to their safety and soundness standards.

The NCUA Board has determined that it can best meet the congressional directive to prescribe standards through an amendment to NCUA's existing regulation governing security programs in federally-insured credit unions. The proposed regulation will require that federally-insured credit unions establish a security program addressing the safeguards required by the GLB Act. The Board also proposes to publish an appendix to the regulation that will set out guidelines, the text of which is substantively identical to the guidelines anticipated from the federal banking agencies. The guidelines are intended to outline industry best practices and assist credit unions to develop meaningful and effective security programs to ensure their compliance with the safeguards contained in the regulation.

Currently, NCUA regulations require that federally-insured credit unions have a written security program designed to protect each credit union from robberies, burglaries, embezzlement, and assist in the identification of persons who attempt such crimes. Expanding the environment of protection to include threats or hazards to member information systems is a natural fit within a comprehensive security program.
To evaluate compliance, the NCUA will expand its review of credit union security

programs and annual certifications. This review will take place during safety and soundness examinations for federal credit unions and within the established oversight procedures for state-chartered, federally-insured credit unions. If a credit union fails to establish a security program meeting the regulatory objectives, the NCUA Board could take a variety of administrative actions. The Board could use its cease and desist authority, including its authority to require affirmative action to correct deficiencies in a credit union's security program. 12 U.S.C. 1786(e) and (f). In addition, the Board could employ its authority to impose civil money penalties. 12 U.S.C. 1786(k). A finding that a credit union is in violation of the requirements of proposed §748.0(b)(2) would typically result only if a credit union fails to establish a written policy or its written policy is insufficient to reasonably address the objectives set out in the proposed regulation.

The proposed Guidelines apply to "nonpublic personal information" of "members" as those terms are defined in 12 CFR Part 716, the Privacy Rule. Under Section 503(b)(3) of the GLB Act and part 716, credit unions will be required to disclose their policies and practices with respect to protecting the confidentiality, security, and integrity of nonpublic personal information as part of the initial and annual notices to their members. Defining terms consistently should facilitate the ability of credit unions to develop their privacy notices in light of the guidelines set forth here. NCUA derived key components of the proposed Guidelines from security-related supervisory guidance developed with the federal banking agencies through the Federal Financial Institutions Examination Council (FFIEC).

The NCUA Board requests comment on all aspects of the proposed amendment of §748.0 and the guidelines, as well as comment on the specific provisions and issues highlighted in the section-by-section analysis below.

II. Section-by-Section Analysis

The discussion that follows applies to the proposed rule Part 748.

The security program in §748.0(b) previously addressed only those threats due to acts such as robberies, burglaries, larcenies, and embezzlement. In the emerging electronic marketplace, the threats to members, credit unions, and the information they share to have a productive, technologically competitive, financial relationship, have increased. The security programs to ensure protections against these emerging crimes and harmful actions must keep pace. Congress directed in Section 501(b) of the GLB Act that the Agencies establish standards to ensure financial institutions protect the security and confidentiality of the nonpublic personal information of its customers.

To meet this directive, the proposed rule revises paragraph (b) of §748.0 to require that a credit union's security program include protections to ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use

of such records that could result in substantial harm or inconvenience to a member. This modification expands the security program objectives to include the emerging threats and hazards to members, credit unions, and the information they share to have a financial relationship.

The proposed rule would have an effective date of November 13, 2000; however, compliance would not be required until July 1, 2001. This is consistent with Part 716, the Privacy Rule, and the other Agencies. NCUA intends to maintain its 90-day compliance period for newly-chartered or insured credit unions found in §748.0(a). This section requires that each credit union establish its written security program within 90 days from the date of insurance. While the GLB Act, and the other Agencies regulations are silent as to compliance for newly chartered or insured institutions, NCUA believes it is reasonable to continue to provide this compliance time frame for such credit unions.

The discussion that follows applies to the NCUA's proposed Guidelines.

APPENDIX A TO PART 748 – GUIDELINES FOR SAFEGUARDING MEMBER INFORMATION

I. Introduction

Proposed paragraph I. sets forth the general purpose of the proposed Guidelines, which is to provide guidance to each credit union in establishing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information. This paragraph also sets forth the statutory authority for the proposed Guidelines, sections 501 and 505(b) of the GLB Act. 15 U.S.C. 6801 & 6805(b).

I.A. Scope

Paragraph I.A. describes the scope of the proposed Guidelines. The proposed Guidelines can apply to all federally-insured credit unions.

I.B. Definitions

Paragraph I.B. sets forth the definitions of various terms for purposes of the proposed Guidelines.

I.B.1. In general

Paragraph I.B.1. provides that terms used in the proposed Guidelines have the same meanings as set forth in 12 CFR Part 716, except to the extent that the definition of the term is modified in the proposed Guidelines or where the context requires otherwise.

I.B.2. Member information

Proposed paragraph I.B.2. defines member information. Member information includes any records, data, files, or other information about a member containing nonpublic personal information, as defined in 12 CFR §716.3(q). This includes records in paper, electronic, or any other form that are within the control of a credit union or that are maintained by any service provider on behalf of a credit union. Although the GLB Act uses both the terms “records” and “information,” for the sake of simplicity, in the proposed Guidelines the term “records” encompasses all member information.

Section 501(b) refers to safeguarding the security and confidentiality of “customer” information. The term “customer” is also used in other sections of Title V of the GLB Act. The NCUA Board has used the term “member” in place of the term “customer” in implementing these sections of the GLB Act in Part 716. The term “member” includes individuals who are not actually members, but are entitled to the same privacy protections under Part 716 as members. Examples of individuals that fall within the definition of member in Part 716 are nonmember joint account holders, nonmembers establishing an account at a low-income designated credit union, and nonmembers holding an account in a state-chartered credit union under state law. The term “member” does not cover business members, or consumers who have not established an ongoing relationship with the credit union (e.g., those consumers that merely use an

ATM or purchase travelers checks). See 12 CFR §§716.3(n) and (o).

The NCUA Board proposes defining "member" for purposes of the Guidelines consistently with Part 716 to facilitate the ability of a credit union to develop the privacy notices and to make disclosures required under Section 503(b)(3). However, the NCUA Board is considering whether the scope of the Guidelines should address records for all consumers, the credit union's business account holders, or all of a credit union's records. The NCUA Board solicits comment on whether a broader definition will change the information security program that a credit union would implement, or, whether, as a practical matter, credit unions will respond to the Guidelines by implementing an information security program for all types of records under their control rather than segregating "member" records for special treatment.

I.B.3. Member

Proposed paragraph I.B.3. defines member to include any member of a credit union as defined in 12 CFR §716.3(n). A member is a consumer who has established a continuing relationship with a credit union under which the credit union provides one or more financial products or services to the member to be used primarily for personal, family or household purposes.

I.B.4. Service provider

Proposed paragraph I.B.4. defines a service provider as any person or entity that maintains or processes member information on behalf of a credit union, or is otherwise granted access to member information through its provision of services to a credit union.

I.B.5. Member information system

Proposed paragraph I.B.5. defines member information system to be electronic or physical methods used to access, collect, store, use, transmit, and protect member information.

II. Standards for Safeguarding Member Information

II.A. Information Security Program

The proposed Guidelines describe NCUA's expectations for the creation, implementation, and maintenance of an information security program. The proposed Guidelines first describe the oversight role of the board of directors in this process and management's continuing duty to evaluate and report to the credit union's board on the overall status of the program. The proposed Guidelines proceed to describe a four-step information security program that: (1) identifies and assesses the risks that may

threaten member information; (2) develops a written plan containing policies and procedures to manage and control these risks; (3) implements and tests the plan; and (4) adjusts the plan on a continuing basis to account for changes in technology, the sensitivity of member information, and internal or external threats to information security.

Lastly, the proposed Guidelines describe responsibilities for overseeing outsourcing arrangements.

Proposed paragraph II.A. sets forth the general requirement in section 501 of the GLB Act that each credit union have a comprehensive information security program. This program is to include administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities.

II.B. Objectives

Proposed paragraph II.B. describes the objectives for an information security program. They are to ensure the security and confidentiality of member information, protect against any anticipated threats or hazards to the security or integrity of such information, and protect against unauthorized access to or use of member information that could either: (1) result in substantial harm or inconvenience to any member; or (2) present a safety and soundness risk to the credit union.

Unauthorized access to or use of member information does not include access to or use of member information with the member's consent. The NCUA Board requests comment on whether there are additional or alternative objectives that should be included in the Guidelines.

III. Development and Implementation of Information Security Program

III.A. Involve the Board of Directors and Management

Proposed paragraph III.A. describes the involvement of the board and management in the development and implementation of an information security program. This paragraph specifies these board responsibilities: (1) approve the credit union's written information security policy and program; and (2) oversee efforts to develop, implement, and maintain an effective information security program, including the regular review of management reports.

The proposed Guidelines set forth three responsibilities for management as part of its implementation of the credit union's information security program. The first provision recognizes the need for an ongoing assessment of changes in technology and their impact on the credit union, as appropriate. On a regular basis, management has a responsibility to evaluate the impact on the credit union's security program of changing

business arrangements (e.g. alliances, joint ventures, or outsourcing arrangements), and changes to member information systems.

The second provision describes management's responsibility to document compliance with these Guidelines.

The third responsibility of management is to keep the credit union's board of directors informed of the current status of the credit union's information security program. On a regular basis, management should report to the board on the overall status of the information security program, including material matters related to: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements to the information security program.

The NCUA Board invites comment as to whether the Guidelines should provide that in some instances the credit union's board of directors should designate an Information Security Officer or other responsible individual who would have the authority, subject to the board's approval, to develop and administer the credit union's information security program. The NCUA Board also invites comment on what best practices or business models would be most appropriate for the assignment of these tasks, depending upon the size and complexity of the credit union.

The NCUA Board invites comment regarding the appropriate frequency of reports to the credit union's board of directors. Should the Guidelines specify best practices for reporting intervals – monthly, quarterly, or annually? How often should management report to the credit union's board of directors regarding the credit union's information security program and why are these intervals appropriate?

III.B. Assess Risk

Proposed paragraph III.B. describes the risk assessment process that should be developed as part of the information security program. First, as described in paragraph III.B.1, a credit union should identify and assess risks that may threaten the security, confidentiality, or integrity of member information, whether in storage, processing, or transit. The risk assessment should be made in light of a credit union's operations and technology. A credit union should determine the sensitivity of member information to be protected as part of this analysis.

Next, as described in paragraph III.B.2, a credit union should conduct an assessment of the sufficiency of existing policies, procedures, member information systems, and other arrangements intended to control the risks identified under III.B.1.

Finally, as described in paragraph III.B.3, a credit union should monitor, evaluate, and adjust, their risk assessments, taking into consideration any technological or other

changes or the sensitivity of the information.

III.C. Manage and Control Risk

Proposed paragraph III.C describes the elements of a comprehensive risk management plan designed to control identified risks and to achieve the overall objective of ensuring the security and confidentiality of member information. Paragraph 1 identifies the factors a credit union should consider in evaluating the adequacy of its policies and procedures to effectively manage these risks commensurate with the sensitivity of the information as well as the complexity and scope of the credit union and its activities. Specifically, a credit union should consider whether its risk management program includes appropriate:

a) access rights to member information;
b) access controls on member information systems, including controls to authenticate and grant access only to authorized individuals and companies;
c) access restrictions at locations containing member information, such as buildings, computer facilities, and records storage facilities;
d) encryption of electronic member information, including, while in transit or in storage on networks or systems to which unauthorized individuals may have access;
e) procedures to confirm that member information system modifications are consistent with the credit union's information security program;

f) dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information;
g) contract provisions and oversight mechanisms to protect the security of member information maintained or processed by service providers;
h) monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems;
i) response programs that specify actions to be taken when unauthorized access to member information systems is suspected or detected;
j) protection against destruction of member information due to potential physical hazards, such as fire and water damage; and
k) response programs to preserve the integrity and security of member information in the event of computer or other technological failure, including, where appropriate, reconstructing lost or damaged member information.

The NCUA Board intends that these elements accommodate credit unions with varying operations and risk management structures. The NCUA Board invites comment on the degree of detail that should be included in the Guidelines regarding the risk management program, which elements should be specified in the Guidelines, and any other components of a risk management program that should be included.

Paragraph 2 refers to staff training. The information security program should include a training component designed to teach employees to recognize and respond to

fraudulent attempts to obtain member information and report any attempts to regulatory and law enforcement agencies.

Paragraph 3 refers to testing procedures. An information security program should include regular testing of systems to confirm the credit union, and its service providers, control identified risks and achieve the objectives to ensure the security and confidentiality of member information. The NCUA Board invites comment on whether the Guidelines should address specific types of security tests, such as penetration tests or intrusion detections tests. Should there be a degree of independence in connection with the testing of information security systems and the review of test results. Should the tests or reviews of tests be conducted by persons who are not employees or volunteers of the credit union? If employees, or volunteers such as members of the credit union's supervisory committee, what measures, if any, are appropriate to assure their independence?

Paragraph 4 describes the need for an ongoing process of monitoring, evaluation, and adjustment of the information security program in light of any relevant changes in technology, the sensitivity of member information, and internal or external threats to information security.

III.D. Oversee Outsourcing Arrangements

Proposed paragraph III.D addresses outsourcing. A credit union should exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect member information and member information systems consistent with these Guidelines.

The NCUA Board welcomes comments on the appropriate treatment of outsourcing arrangements. For example, which "best practices" most effectively monitor service provider compliance with security precautions? Do service providers accommodate requests for specific contract provisions regarding information security? To the extent that service providers do not accommodate these requests, how does a credit union implement an effective information security program? Should these Guidelines contain specific contract provisions for service provider performance standards in connection with the security of member information?

III. Regulatory Procedures

A. Paperwork Reduction Act

The NCUA Board has determined that the proposed information security plan requirements in are covered under the Paperwork Reduction Act. NCUA is submitting a copy of this proposed rule to the Office of Management and Budget (OMB) for its review.

The proposed amendment would require federally-insured credit unions to develop a written information security plan to protect the security, confidentiality, or integrity of member information systems. The Board estimates it will take an average of 40 hours for a credit union to comply with the information security plan requirement. The Board also estimates that 10,525 credit unions will have to develop this plan so the total initial paperwork burden is estimated to be approximately 421,000 hours. The estimate of annual burden of review and changes is 15 hours for 10,500 credit unions, totaling 157,500.

The Paperwork Reduction Act of 1995 and OMB regulations require that the public be provide an opportunity to comment on the paperwork requirements, including an agency's estimate of the burden of the paperwork requirements. The NCUA Board invites comment on: (1) whether the paperwork requirements are necessary; (2) the accuracy of NCUA's estimate on the burden of the paperwork requirements; (3) ways to enhance the quality, utility, and clarity of the paperwork requirements; and (4) ways to minimize the burden of the paperwork requirements. Comments should be sent to: OMB Reports Management Branch, New Executive Office Building, Room 10202, Washington, D.C. 20503; Attention: Alex T. Hunt, Desk Officer for NCUA. Please send NCUA a copy of any comments you submit to OMB.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act (5 U.S.C. §§ 601-612) (RFA) requires an agency to publish an initial regulatory flexibility analysis with this proposed rule except to the extent provided in the RFA, whenever the agency is required to publish a general notice of proposed rulemaking for a proposed rule. The Board cannot at this time determine whether the proposed rule would have significant economic impact on a substantial number of small entities as defined by the RFA. Therefore, pursuant to subsections 603(b) and (c) of the RFA, the Board provides the following initial regulatory flexibility analysis.

1. Reasons for Proposed Rule

The NCUA is requesting comment on the proposed interagency Guidelines published pursuant to section 501 of the GLB Act. Section 501 requires the Agencies to publish standards for financial institutions relating to administrative, technical, and physical standards to: (1) insure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. Since these requirements are expressly mandated by the GLB Act, it is the view of the Board that the GLB Act's requirements account for most, if not all, of the economic impact of the proposed Guidelines.

2. Statement of Objectives and Legal Basis

The **Supplementary Information** section above contains this information. The legal basis for the proposed rule is the GLB Act.

3. Estimate of Small Credit Unions to Which the Rule Applies

The proposed rule would apply to all federally insured credit unions. Small credit unions are those with less than $1,000,000 in assets of which there are approximately 1,624.

4. Projected Reporting, Recordkeeping and Other Compliance Requirements

The information collection requirements imposed by the proposed rule are discussed above in the section on the Paperwork Reduction Act.

5. General Requirements

The statute and the proposed rule require a credit union to develop an information security program to safeguard member information. Development of such a program involves assessing risks to member information, establishing policies, procedures, and training to control risks, testing the program's effectiveness, and

managing and monitoring service providers. The NCUA believes that the establishment of information security programs is a sound business practice for a credit union and is already addressed by existing supervisory procedures. However, some credit unions may need to establish or enhance information security programs, but the cost of doing so is not known. The NCUA seeks any information or comment on the costs of establishing information security programs.

1. Identification of Duplicative, Overlapping, or Conflicting Federal Rules

The NCUA is unable to identify any statutes or rules which would overlap or conflict with the requirement to develop and implement an information security program. The NCUA seeks comment and information about any such statutes or rules, as well as any other state, local, or industry rules or policies that require a credit union to implement business practices that would comply with the requirements of the proposed rule.

7. Discussion of Significant Alternatives

As previously noted, the proposed rule's requirements are expressly mandated by the GLB Act. The proposed rule attempts to clarify the statutory requirements for all credit unions. The proposed rule also provides substantial flexibility so that any credit union, regardless of size, may adopt an information security program tailored to its

individual needs. The NCUA welcomes comment on any significant alternatives, consistent with the GLB Act, that would minimize the impact on small credit unions.

C. Executive Order 13132

Executive Order 13132 encourages independent regulatory agencies to consider the impact of their regulatory actions on state and local interests. In adherence to fundamental federalism principles, NCUA, an independent regulatory agency as defined in 44 U.S.C. 3502(5), voluntarily complies with the executive order. This proposed rule, if adopted, will not have substantial direct effects on the states, on the relationship between the national government and the states, or on the distribution of power and responsibilities among the various levels of government. NCUA has determined the proposed rule and appendix does not constitute a policy that has federalism implications for purposes of the executive order.

D. Treasury and General Government Appropriations Act, 1999

NCUA has determined that the proposed rule and appendix will not affect family well-being within the meaning of section 654 of the Treasury and General Government Appropriations Act, 1999, Pub. L. 105-277, 112 Stat. 2681 (1998).

IV. Agency Regulatory Goal

NCUA's goal is clear, understandable regulations that impose minimal regulatory burden. NCUA requests comments on whether the proposed rule and appendix are understandable and minimally intrusive if implemented as proposed. NCUA invites comments on how to make this proposal easier to understand. For example:

(1) Has NCUA organized the material to suit your needs? If not, how could this material be better organized?
(2) Are the provisions in the Guidelines clearly stated? If not, how could the Guidelines be more clearly stated?
(3) Do the Guidelines contain technical language or jargon that is not clear? If so, which language requires clarification?
(4) Would a different format (grouping and order of sections, use of headings, paragraphing) make the Guidelines easier to understand? If so, what changes to the format would make the Guidelines easier to understand?
(5) What else could NCUA do to make the Guidelines easier to understand?

List of Subjects

12 CFR Part 716

Consumer protection, Credit unions, Privacy, Reporting and recordkeeping

requirements.

12 CFR Part 748

Credit unions, Crime, Currency, Reporting and recordkeeping requirements and Security measures.

By the National Credit Union Administration Board on June 6, 2000.

_____

Becky Baker

Secretary of the Board

For the reasons set forth in the preamble, the NCUA Board proposes to amend 12 CFR 748 as follows:

PART 748—Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance.

1. The authority citation for Part 748 is revised to read as follows:

Authority: 12 U.S.C. 1766(a), 1786(Q); 15 USC 6801 and 6805(b); 31 USC 5311.

2. Heading for Part 748 is revised as set forth above.

3. In §748.0 revise paragraph (b) to read as follows:

§748.0 Security program.

* * * * * *

(b) The security program will be designed to:

(1) protect each credit union office from robberies, burglaries, larcenies, and embezzlement;

(2) ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;

(3) assist in the identification of persons who commit or attempt such actions and crimes; and

(4) prevent destruction of vital records, as defined in the *Accounting Manual for Federal Credit Unions.*

4. Add Appendix A to read as follows:

Appendix A to Part 748 -- Guidelines for Safeguarding Member Information

Table of Contents

I. Introduction

The Guidelines for Safeguarding Member Information (Guidelines) set forth standards pursuant to sections 501and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines provide guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the

security, confidentiality, and integrity of member information.

A. Scope. The Guidelines apply to member information maintained by or on behalf of federally-insured credit unions. Such entities are referred to in this appendix as "the credit union."

B. Definitions. For purposes of the Guidelines, the following definitions apply:

1. In general. For purposes of the Guidelines, except as modified in the Guidelines or unless the context otherwise requires, the terms used have the same meanings as set forth in 12 CFR Part 716.

2. Member information means any records, data, files, or other information containing nonpublic personal information, as defined in 12 CFR §716.3(q), about a member, whether in paper, electronic or other form, that are maintained by or on behalf of the credit union.

3. Member means any member of the credit union as defined in 12 CFR §716.3(n).

4. Service provider means any person or entity that maintains or processes member information on behalf of the credit union, or is otherwise granted access to

member information through its provision of services to the credit union.

5. Member information systems means the electronic or physical methods used to access, collect, store, use, transmit and protect member information.

II. Guidelines for Safeguarding Member Information

A. Information Security Program. A comprehensive information security program includes administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities.

B. Objectives. An information security program: (1) ensures the security and confidentiality of member information; (2) protects against any anticipated threats or hazards to the security or integrity of such information; and (3) protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member or risk to the safety and soundness of the credit union.

Protecting confidentiality includes honoring members' requests to opt out of disclosures to non-affiliated third parties, as described in Part 716.1(a)(3).

III. Development and Implementation of Information Security Program

A. Involve the Board of Directors and Management.

1. The board of directors of each credit union:

a. approves the credit union's written information security policy and program; and

b. oversees efforts to develop, implement, and maintain an effective information security program.

2. In conjunction with responsibilities to implement the credit union's information security program, management should regularly:

a. evaluate the impact on the credit union's security program of changing business arrangements, such as alliances and, outsourcing arrangements, and changes to member information systems;

b. document its compliance with these Guidelines; and

c. report to the board of directors on the overall status of the information security program, including material matters related to: risk assessment; risk management and control decisions; results of testing; attempted or actual security breaches or violations and responsive actions taken by management; and any recommendations for improvements in the information security program.

B. Assess Risk. To achieve the objectives of its information security program, credit

unions should:

1. Identify and assess the risks that may threaten the security, confidentiality, or integrity of member information systems. As part of the risk assessment, a credit union should determine the sensitivity of member information and the internal or external threats to the credit union's member information systems;

2. Assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks identified above; and

3. Monitor, evaluate, and adjust its risk assessment in light of any relevant changes to technology, the sensitivity of member information, and internal or external threats to information security.

C. Manage and Control Risk. As part of a comprehensive risk management plan, each credit union should:

1. Establish written policies and procedures that are adequate to control the identified risks and achieve the overall objectives of the credit union's information security program. Policies and procedures should be commensurate with the sensitivity of the information as well as the complexity and scope of the credit union and its activities. In establishing the policies and procedures, each credit union should consider appropriate:

a. access rights to member information;

b. access controls on member information systems, including controls to

authenticate and grant access only to authorized individuals and companies;

c. access restrictions at locations containing member information, such as buildings, computer facilities, and records storage facilities;

d. encryption of electronic customer information, including, while in transit or in storage on networks or systems to which unauthorized individuals may have access;

e. procedures to confirm that member information system modifications are consistent with the credit union's information security program;

f. dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information;

g. contract provisions and oversight mechanisms to protect the security of member information maintained or processed by service providers;

h. monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems;

i. response programs that specify actions to be taken when unauthorized access to member information systems is suspected or detected;

j. protection against destruction of member information due to potential physical hazards, such as fire and water damage; and

k. response programs to preserve the integrity and security of member information in the event of computer or other technological failure,

including, where appropriate, reconstructing lost or damaged member information.

2. Train staff to recognize, respond to, and, where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain member information.

3. Regularly test the key controls, systems and procedures of the information security program to confirm that they control the risks and achieve the overall objectives of the credit union's information security program. The frequency and nature of such tests should be determined by the risk assessment, and adjusted as necessary to reflect changes in internal and external conditions. Tests should be conducted, where appropriate, by independent third parties or staff independent of those that develop or maintain the security programs. Test results should be reviewed by independent third parties or staff independent of those whom conducted the test.

4. Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its member information, and internal or external threats to information security.

D. Oversee Outsourcing Arrangements. The credit union continues to be responsible for safeguarding member information even when it gives a service provider access to

that information. The credit union should exercise appropriate due diligence in managing and monitoring its outsourcing arrangements to confirm that its service providers have implemented an effective information security program to protect member information and member information systems consistent with these Guidelines.